CYBERVICTIMIZATION

Jeri N. Roberts
Tina Jaeckle
Thomas A. Petee
John P. Jarvis

One aspect of computer crime that has been underdeveloped in the cybercrime literature is victimization. More specifically, there has been a paucity of information on the victimology of cybercrime – characteristics and demographics on those individuals and organizations that are victimized by cybercriminals. Do they look like the victims of conventional crime, or are they different in some respects? Moreover, as the cyber landscape continues to evolve, will victim characteristics change to any significant degree?

TYPES OF CYBERVICTIMIZATION

The nature and variety of victimization with cybercrime in some ways parallels the complexity we see with conventional criminality. A long standing distinction has often been made in criminology between *crimes against persons* and *crimes against property*. That same distinction can be made with computer-related crime, although there are some unique elements that occur with cybercrime that blur that distinction and which may change the nature of criminal victimization in the future.

Personal Forms of Cybercrime

Crimes against persons, or personal crimes, usually involve situations where the offender uses some conception of force or coercion against a victim. What constitutes "force" for these offenses is somewhat flexible but commonly will involve a physical element. Consequently, "crimes against persons" is sometimes used interchangeably with "violent crime", although they are not fully synonymous. With conventional criminality, there is a notion that personal crimes require a certain degree of propinquity between the offender and victim, as is the case with most instances of crimes such as assault, murder, rape or kidnapping. Although there are exceptions (e.g., a situation where a sniper shoots a victim at some significant distance), the vast majority of these types of personal crime do involve direct contact between the offender and the victim. Computer-related crime, almost by its very nature, can be devoid of this type of physical contact. A cybercriminal can use computer technology in such a way as to at least initially remove him/herself from direct contact with the victim. Consequently, personal cybercrime to some degree becomes a misnomer, so that these offenses could be almost described as "impersonal" personal crimes.

There are a wide variety of behaviors that could be classified as personal cybercrime, ranging from relatively minor vandalism-type offenses to more serious, threatening behavior. More specifically, there are a number of personal forms of cybercrime which have generated a good deal of attention:

● Cyberstalking: generally defined as the use of the internet, e-mail or other electronic communication devices to repeatedly harass or threaten an

individual (Department of Justice, 1999). Some experts view cyberstalking as an extension of offline stalking – a preexisting problem exacerbated by technology (Ellison & Akdeniz, 1998).

● Online threat-related extortion: where an offender uses threats sent through e-mail in order to extort money from the victim.

● Disruption of services: where individuals are targeted for the disruption of computer-related telecommunication services through techniques such as mass spamming or the transmission of computer viruses.

● Online sexual predation: primarily situations where pedophiles and other sexual predators solicit underage children online, usually in chat rooms (see, for example, any of the cases featured on Dateline NBC's "To Catch a Predator" series).

The volume of personal cybercrime victimization is likely to increase in the coming years. As more and more people gain access to computers, and particularly to online forms of communication, they will find themselves at risk for being victimized by some form of personal cybercrime. The popularity of chat rooms, instant messaging and other online communication forms increase the likelihood of exposure to potential victimization by predatory individuals.

Economic and Property-related Cybercrime

Crimes against property usually involve situations where the victim suffers some type of economic loss or property damage. Economic loss can be something that is tangible, as with most situations classified as theft, or more abstract, as would be the case with the loss of productivity resulting from criminal activity. Property damage certainly involves an economic element but is usually related to the replacement or restoration of the damaged property.

With cybercrime, property-related offenses encompass many of the same types of behavior seen with more conventional types of crime but involve the use of computer technology to facilitate the offense, often in new and innovative ways:

● Phishing: "Phishing" is a general term for criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords. The "phishers" then take that information and use it for criminal purposes, such as identity theft and fraud (Department of Justice, 2007).

● Identity Theft and Identity Fraud: Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or

deception, typically for economic gain (Department of Justice, 2007a)

● Hacking: Hacking is a term used to describe situations where a secure computer system is breached and perhaps altered. The best analogy in conventional crime for hacking would be criminal trespass and vandalism.

● Cloned Websites: This usually involves the creation of a mirror version of an authorized website, where internet users are lured into the cloned website believing that they are entering the actual authorized website. Information obtained from the users (i.e., credit card information or personal identifiers) can then be used for fraudulent purposes.

● 419 Scams: The "419" in the name of this type of cybercrime refers to Section 419 of the Nigerian Criminal Code. This is a reworking of the classic "bait and hook" scheme where the e-mail recipient is lured into providing personal information such as bank account numbers with the promise that they will be given a share of millions of dollars if they help the sender move funds out of the country. The 419 scams typically depend on the greed of the e-mail recipient, although they sometimes also prey on the goodwill of the intended victim by framing their story around some catastrophic event (e.g., the source claims to have recently lost his/her parents, or alleges that they are dying of some disease). There numerous variations on this scam, with more recent examples seemingly originating from the United Kingdom.

● Hijacked Websites- This type of cybercrime involves situations where attempts to view a website (most commonly a popular webpage or a search engine) are redirected to an alternative website designated by the hijacker without the consent of the user. There are any number of motivations for this type of offense, most frequently those associated with hacking and computer-related fraud, but recent incidents include hijacking perpetrated for political retaliation, such as the case in 2007 where Chinese hackers hijacked several popular search engines and redirected them to Chinese websites after President Bush warmly welcomed the Dalai Lama to the United States.

All of these exploits noted above both continue to be descriptive of the nature of cybervictimizations today and will likely continue into the foreseeable future. The character of these victimizations may change, but the use and exploitation of individuals that utilize computing devices is a virtual certainty that law enforcement and the communities they serve will confront in the future.

References

Department of Justice. (2007a). *Identity theft and fraud.* Retrieved September 27, 2007, from http://www.usdoj.gov/criminal/fraud/websites/idtheft.html.

Department of Justice. (2007b). *Special report on "phishing."* Retrieved September 27, 2007, from

http://www.usdoj.gov/criminal/fraud/docs/phishing.pdf.

Department of Justice. (1999). Report on cyberstalking. Cyberstalking: A new challenge for law enforcement and industry. A report from the Attorney General to the Vice President. Retrieved September 27, 2007, from http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

Ellison, L., & Akdeniz, Y. (1998). Cyber-stalking: The regulation of harassment on the Internet. *Criminal Law Review, Special Edition: Crime, Criminal Justice and the Internet*, 29-48.